AO 91 (Rev. 02/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of New York

United States of America)
v.)
) Case No. 5:16-MJ- 462 (DEP)
Joseph M. Gill)
)

Defendant

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of _____ in the county of Oneida in the Northern District of New York, the defendant violated 18 U. S. C. § 2252A(a)(2)(A), an offense described as follows:
Betweeen on or about June 5, 2015 and on or about March 24, 2016, did knowingly receive child pornography using a means and facility of interstate and foreign commerce in and affecting such commerce.

This criminal complaint is based on these facts:

See attached Affidavit.

☑ Continued on the attached sheet.

Complainant's signature

FBI Special Agent Douglas Soika
Printed name and title

Sworn to before me and signed in my presence.

Date: 09/09/2016

Judge's signature

City and state: Syracuse, New York

Hon. David E. Peebles, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Douglas Soika, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the FBI since August 2005 and am currently assigned to the Albany Division, Utica Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training by the FBI and everyday work relating to conducting these types of investigations. I have also been the Affiant for and participated in the execution of several federal search warrants in child sexual exploitation investigations.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for a criminal complaint charging Joseph Gill with violations of Title 18, United States Code, Section 2252A(a)(2)(A) (receiving child pornography).

4. The information contained in this affidavit is based upon information gathered by me as a part of the investigation as well as information provided to me by other Special Agents of the FBI and other law enforcement officers involved in this investigation. Since this affidavit is being submitted for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that Joseph Gill has committed violations of Title 18, United States Code, Section 2252A(a)(2)(A), as outlined above.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. § 2252A, relating to material involving the sexual exploitation of minors.

a. 18 U.S.C. § 2252A(a)(1) prohibits knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.

b. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

c. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use

of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

c. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. § 1030(e)(1).

d. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software,

documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

i. "Minor" means any person under the age of 18 years. See 18 U.S.C. § 2256(1).

j. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, see 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, see 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. See 18 U.S.C. § 2256(2)(A).

k. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

l. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks,

printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

7. Based on my knowledge, training, and experience, and the experience and training of other law enforcement officers I know that computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

8. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

10. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access

to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

12. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

13. The latest evolution of peer-to-peer file-sharing (P2P), and the version of P2P that was used in this investigation, allows a user to set up his own private P2P network of contacts. File-sharing through this and publicly available P2P file-sharing program is limited only to other users who have been added to a private list of "friends." A new user is added to a list of friends by request. Acceptance of a friend request will allow that new user to download files from the user who sent the friend request. The new user can then browse the list of files that the other user has made available to download, select desired files from this list, and download the selected files. The downloading of a file occurs through a direct connection between the computer requesting the file and the computer containing the file.

14. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time.

15. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

16. Third-party software is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

BACKGROUND OF THE INVESTIGATION

17. On 06/05/2015, an FBI Online Covert Employee (OCE) using a computer connected to the Internet launched a publicly available P2P file sharing program. The OCE identified a user on a P2P file sharing program utilizing an IP address previously associated by Internet Crimes Against Children Investigators as having recently broadcast a file depicting suspected child pornography and located in the state of New York with one file of investigative interest.

18. During the investigation, the computer utilizing the above referenced IP address, 67.241.58.75, reported its nickname as **anon_43f13a4b@Ares**.

19. From 4:48 pm to 6:17 pm, on 06/05/2015, one of the files that the computer at IP address 67.241.58.75 was making available was successfully downloaded. From 3:50 pm to 5:26 pm on 06/08/2015, another file that the computer at IP address 67.241.58.75 was making available was successfully downloaded. The computer at IP address 67.241.58.75 was the sole source for these downloads and, as such, the entire file for each download was taken directly from said IP address.

20. Your affiant has reviewed the downloaded files. They are available for the Court's inspection upon request, and are described as follows:

a) **yamad fuck pthc crimea kingpass p101 zz fkk (2)(2)(2).mpg** – A video file depicting a nude pubescent male child and a nude male. The video file depicts the pubescent child and male masturbating, engaged in anal sex with each other, and performing oral sex on each other.

b) **pthc blowjob (268).jpg** – A picture file depicting a shirtless, pubescent, brown haired child with his/her mouth touching the penis of an adult male.

21. A search of the ARIN online database indicated that IP address 67.241.58.75 is registered to Time Warner Cable. Results from an administrative subpoena sent to Time Warner Cable on 8/20/2015 revealed that on the date and time the files were downloaded by the OCE, IP address 67.241.58.75 was assigned to the account registered to Joe Gill, 161 Pine Haven Circle, Blossvale, New York. The Time Warner Cable account also includes an email address of chevyranger1984@twcny.rr.com, and a telephone number of 315-766-XXXX.

22. On 03/24/2016, an FBI OCE using a computer connected to the Internet, launched a publicly available P2P file sharing program. The OCE identified a user on the P2P file sharing program utilizing an IP address previously associated by Internet Crimes Against Children Investigators as having recently broadcast a file depicting suspected child pornography and located in the state of New York with two files of investigative interest.[1]

23. During the investigation, the computer utilizing the above referenced IP address, 67.241.58.75, reported its nickname as **_cow@Ares**. (Ares is a P2P file sharing program).

24. From 7:49 pm to 11:23 pm on 03/24/2016, two files that the computer at IP address 67.241.58.75 was making available for sharing were successfully downloaded. The computer at

[1] A file "of investigative interest" is a file whose properties include a hash value known to be associated with child pornography.

IP address 67.241.58.75 was the sole source for these downloads and, as such, the entire file for each download was taken directly from said IP address.

25. Your affiant has reviewed the downloaded files. They are available for the Court's inspection upon request, and are described as follows:

a) **toddler being fucked by man 78678(2)(2)(2)(2).mpg** – A video file depicting a nude pre-pubescent child engaged in anal intercourse with an adult male.

b) **((hussyfan)) mylola info sasha2 hard(2).avi** – A video file depicting a nude pubescent female child. The video file depicts the penetration of the vagina of the child by a foreign object.

26. A search of the American Registry for Internet Numbers (ARIN) online database indicated that IP address 67.241.58.75 is registered to the Internet Service Provider Time Warner Cable. According to ARIN's website, ARIN is a nonprofit organization responsible for managing the Internet numbering resources for North America, and a portion of the Caribbean. Results from an administrative subpoena sent to Time Warner Cable on 6/17/2016 revealed that on the date and time the files were downloaded by the OCE, IP address 67.241.58.75 was assigned to the account registered to Joe Gill, 161 Pine Haven Circle, Blossvale, New York (Oneida County). The Time Warner Cable account also includes an email address of chevyranger1984@twcny.rr.com, and a telephone number of 315-766-XXXX.

27. Your affiant has searched various records indices for information on Joe Gill, address 161 Pine Haven Circle, Blossvale, New York. A public records report for Joe Gill, accessed through Accurint, a pay-for service database that can be accessed and searched over the Internet, shows a full name of Joseph M J Gill Jr, and a social security account number XXX-XX-1416, date of birth XX/XX/1955. (The first five digits of the social security account number, and the month and day of the date of birth has been redacted for the purposes of this affidavit.)

28. On 6/13/2016, a physical surveillance of 161 Pine Haven Circle, Blossvale, New York, was conducted. The residence is described as a yellow one-story residence, with a detached car port. (*See* Attachment A.) Your affiant observed a white GMC Envoy, bearing New York registration GTG7792, parked in the property's back yard. New York Department of Motor Vehicle records indicate that the vehicle is registered to Joseph M. Gill Jr, date of birth xx/xx/1955, at 161 Pine Haven Circle, Blossvale, New York. Later that same day, your affiant observed Joe Gill driving the same GMC Envoy away from the 161 Pine Haven Circle address (based on a review of Joe Gill's New York State driver's license photograph and direct observation of the driver of the vehicle.) Additionally, your affiant observed a white Chevy Truck bearing New York registration HBP7727 parked in the detached car port. New York Department of Motor Vehicle records indicate that the vehicle is registered to Joseph M. Gill Jr, date of birth xx/xx/1955, at 161 Pine Haven Circle, Blossvale, New York.

29. On 8/24/2016, your affiant confirmed with the United States Postal Service that Joseph Gill continues to receive mail at the 161 Pine Haven Circle address.

30. On 8/24/2016, your affiant also checked the wireless networks in the area of 161 Pine Haven Circle, which revealed a number of wireless networks, all of which were secured.

31. On 8/22/2016 New York State Police Trooper Brian Hotchkiss responded to a home in the Town of Verona and interviewed a concerned citizen (CC) in regards to a child pornography investigation. During the CC reported that her daughter was residing with a man that lived in the Pine Haven Trailer Park in Rome, NY. The CC further stated that her daughter had called her and advised her that she had located child pornography on this man's laptop computer. CC explained that her daughter described the child pornography as photographs of a child at least five years old.

32. On the same date Trooper Hotchkiss spoke with the CC's daughter over the phone. CC's daughter stated "I am fucking pissed at my mom for telling you this." Trooper Hotchkiss asked CC's daughter to describe what she had discovered on the laptop. CC's daughter stated that she could not provide that information at this time and advised him to call back in about a half an hour. Trooper Hotchkiss stated that it appeared that CC's daughter was in a position to where she felt unsafe to talk to law enforcement at that time over the phone. Trooper Hotchkiss made several attempts to re-contact CC's daughter with negative results.

33. On Monday September 5, 2016 Trooper Hotchkiss re-interviewed CC who advised that she had identified the male that her daughter was living with as Joe Gill. CC advised that her daughter had given her an SD card that was believed to be Gill's and believed to contain child pornography. CC further advised that her daughter had told her that Joe Gill had told CC's daughter that he had destroyed his laptop by throwing it into a canal because he had suspicions that people were starting to suspect he had child pornography on it.

34. On Wednesday September 7, 2016 a New York State Police Investigator reviewed the active files on the SD card provided by CC and determined that no child pornography existed as active files on the card. Further analysis of the SD card is currently being conducted.

SEARCH WARRANT

35. On today's date, your affiant and other law enforcement officials went to Joseph Gill's residence at 161 Pine Haven Circle, Blossvale, New York and executed a search warrant that had been authorized by the Hon. David E. Peebles on September 8, 2016. Gill was present at the time agents arrived to execute the search warrant.

36. Task Force Officer (TFO) Todd Grant interviewed Joseph Gill and showed him the four videos and images that were downloaded by the OCEs from his computer on 03/24/2016 and

06/05/2015 and are referenced above in paragraphs 25 and 20. Your affiant has reviewed these downloaded files. They are available for the Court's inspection upon request, and are described as follows: Downloaded by OCE on 03/24/2016

a) **toddler being fucked by man 78678(2)(2)(2)(2).mpg** – A video file depicting a nude pre-pubescent child engaged in anal intercourse with an adult male.

b) **((hussyfan)) mylola info sasha2 hard(2).avi** – A video file depicting a nude pubescent female child. The video file depicts the penetration of the vagina of the child by a foreign object.

Downloaded by OCE on 06/05/2015

a) **yamad fuck pthc crimea kingpass p101 zz fkk (2)(2)(2).mpg** – A video file depicting a nude pubescent male child and a nude male. The video file depicts the pubescent child and male masturbating, engaged in anal sex with each other, and performing oral sex on each other.

b) **pthc blowjob (268).jpg** – A picture file depicting a shirtless, pubescent, brown haired child with his/her mouth touching the penis of an adult male.

37. After being shown these four videos and images from them Joseph Gill admitted searching for and downloading from the internet 3 of these files and viewing them on his computer. Specifically, Gill admitted to searching for downloading and viewing: **toddler being fucked by man 78678(2)(2)(2)(2).mpg, ((hussyfan)) mylola info sasha2 hard(2),** and **pthc blowjob (268).jpg.** He stated that the computer he used to do this was removed by him from his residence and stored at his sister's house. According to Gill, he moved the computer after being accused of possessing child pornography earlier in the month in an effort to prevent others from accessing his computer. He further stated that he uses the Internet program Ares to search for and obtain child pornography. According to Gill he uses the search terms "pthc[2]," preteen, and Vicky, to obtain

[2] As an investigator I am aware that "pthc", stands for preteen hardcore pornography.

child pornography files. He said after viewing the child pornography he would delete the files. Gill admitted that he has been engaged in this conduct since 2012.

CONCLUSION

38. Based upon the above information, there is probable cause to conclude that Joseph Gill has knowingly received child pornography using a means and facility of interstate and foreign commerce, and in and affecting such commerce, in violation of 18 U.S.C. §§ 2252A(a)(2)(A).

Douglas Soika
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this

9th day of September, 2016

HON. DAVID E. PEEBLES
UNITED STATES MAGISTRATE JUDGE